View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

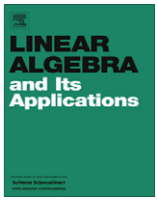
provided by Elsevier - Publisher Connector

Linear Algebra and its Applications 436 (2012) 1258–1266

Contents lists available at SciVerse ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa



Time-domain description of behaviors over finite fields ☆

J.W. Polderman

University of Twente, Department of Applied Mathematics, P.O. Box 217, 7500 AE Enschede, The Netherlands

ARTICLE INFO

Article history:
Received 30 November 2010
Accepted 8 August 2011
Available online 21 October 2011

Submitted by V. Mehrmann

Keywords:
Behavior
Finite field

ABSTRACT

We consider autonomous behaviors over a finite field with characteristic values that do not necessarily belong to the field. The time domain description of the behavior is given in a suitable field extension of the base field. The problem that we consider is how to derive a description completely within the base field. For the case of behaviors over the reals there is a common splitting field for all irreducible polynomials, the complex field. Complex trajectories induce real trajectories by restricting coefficients of complex conjugate exponentials to be complex conjugate as well. For the case of finite fields the situation is more complicated as there does not exist a single finite field extension in which all polynomials over the base field split. In this paper we describe a systematic procedure to obtain explicit expressions for all trajectories in the behavior whose components take values in the base field.

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

Let $p(\xi) \in \mathbb{R}[\xi]$ be a nonzero polynomial with, for ease of discussion, simple roots. The general, real-valued, solution of the difference equation $p(\sigma)w = 0$ is well-known and given by

$$w(k) = \sum_{i=1}^{N} a_i \lambda_i^k, \quad k \in \mathbb{Z}_+.$$

where λ_i, $i = 1, \ldots, N$, are the (distinct) complex roots of $p(\xi)$. The coefficients a_i are elements of $\mathbb{C}$ that come in complex conjugate pairs, that is, if $\bar{\lambda}_i = \lambda_j$ then $\bar{a}_i = a_j$. This ensures that the values $w(k)$ are elements of $\mathbb{R}$. Furthermore $a_i \in \mathbb{R}$ whenever $\lambda_i \in \mathbb{R}$.

☆ A preliminary version of this paper was presented at the MTNS 2008, see [1].

E-mail address: j.w.polderman@math.utwente.nl

0024-3795/$ - see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2011.08.034

We conclude that to derive a general solution of $p(\sigma)w = 0$ with $w\colon \mathbb{Z}_+ \to \mathbb{R}$ we need the extension field $\mathbb{C} = \mathbb{R}(i)$ of $\mathbb{R}$ with $i^2 + 1 = 0$ if $p(\xi)$ does not split in $\mathbb{R}$.

In [2] a theorem is presented that describes the behavior over a finite field $\mathbb{F}$ for the multivariable case, i.e., $P(\xi) \in \mathbb{F}^{q\times q}[\xi]$, and $\det P(\xi)$ splits over $\mathbb{F}$. In this theorem the *Hasse derivative* is used. The jth Hasse derivative of a polynomial matrix $P(\xi) = \sum_{i=0}^{n} p_i\xi^i$ is defined by $D_H^j P(\xi) := \sum_{i=j}^{n} \binom{i}{j} p_i \xi^{i-j}$.

Theorem 1.1 [2, Theorem 2.13]. *Let $P(\xi) \in \mathbb{F}^{q\times q}[\xi]$, let $\det P(\xi)$ be a monic polynomial of degree n, and let $\mathfrak{B} = \{w\colon \mathbb{Z}_+ \to \mathbb{F}^q \mid P(\sigma)w = 0\}$. Then $\mathfrak{B}$ is an n-dimensional subspace of $(\mathbb{F}^q)^{\mathbb{Z}_+}$. If*

$$\det P(\xi) = \prod_{i=1}^{N} (\xi - \lambda_i)^{m_i}$$

with $\lambda_i \in \mathbb{F}$, then all trajectories in $\mathfrak{B}$ are of the form

$$w(k) = \sum_{i=1}^{N} \sum_{j=0}^{m_i-1} b_{ij} D_{\mathrm{H}}^j(\xi^k)\big|_{\xi=\lambda_i} \tag{1}$$

with $b_{ij} \in \mathbb{F}^q$ satisfying the linear restrictions

$$\sum_{j=l}^{m_i-1} \left[D_{\mathrm{H}}^{j-l} P(\xi)\big|_{\xi=\lambda_i}\right] b_{ij} = 0\,, \quad l = 0, \ldots, m_i - 1,\ i = 1, \ldots, N. \tag{2}$$

As we have seen, the behavior $\tilde{\mathfrak{B}} = \{w\colon \mathbb{Z}_+ \to \mathbb{C} \mid p(\sigma)w = 0\}$ with $p(\xi) \in \mathbb{R}[\xi]$ can be explicitly described. By putting restrictions on the coefficients (such that they are complex conjugates), the behavior $\mathfrak{B} = \{w\colon \mathbb{Z}_+ \to \mathbb{R} \mid p(\sigma)w = 0\}$ is obtained.

The question is now whether we can do something similar for Theorem 1.1. Can we define a field extension $\mathbb{E}$ of finite field $\mathbb{F}$ such that $p(\xi)$ splits over $\mathbb{E}$, derive the general solution from Theorem 1.1 for $\mathbb{W} = \mathbb{E}$ and then restrict the coefficients such that the values of all solutions $w(k)$ are elements of $\mathbb{F}$. This problem is discussed in Section 2.

The next question is if we can do this in the multivariable case. This is answered in Section 3.

It is important to note that every polynomial $p(\xi) \in \mathbb{R}[\xi]$ splits over $\mathbb{C}$. $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$. However, for a finite field $\mathbb{F}$ there does not exist a *finite* field extension $\mathbb{E}$ such that every polynomial $p(\xi) \in \mathbb{F}[\xi]$ splits over $\mathbb{E}$. That is why we will define a field extension $\mathbb{E}/\mathbb{F}$ for a given specific polynomial $p(\xi) \in \mathbb{F}[\xi]$, such that $p(\xi)$ splits over $\mathbb{E}$. For a detailed discussion of (finite) splitting fields we refer to [3].

2. The scalar case

In this section we discuss behaviors that are linear subsets of $\mathbb{F}^{\mathbb{Z}_+}$, given by $\mathfrak{B} = \{w\colon \mathbb{Z}_+ \to \mathbb{F} \mid p(\sigma)w = 0\}$. Where $\mathbb{F}$ is a finite field and $p(\xi) \in \mathbb{F}[\xi]$ is a monic polynomial of degree n.

Factorize $p(\xi)$ as

$$p(\xi) = \prod_{i=1}^{N} p_i(\xi)^{m_i}, \tag{3}$$

where $p_i(\xi)$ are the distinct irreducible factors of $p(\xi)$ and m_i their respective multiplicities. If we denote the behaviors corresponding to $p_i(\xi)^{m_i}$ by $\mathfrak{B}_i$, then it is obvious that

$$\mathfrak{B} = \bigoplus_{i=1}^{N} \mathfrak{B}_i. \tag{4}$$

The problem is therefore reduced to behaviors defined by powers of irreducible polynomials. We first analyze the case that $p(\xi)$ is irreducible over $\mathbb{F}$. Since finite fields are perfect (see [3, Theorem 2.14]),

all roots have multiplicity one. In what follows $\mathbb{E}$ is the splitting field of $p(\xi)$, the (distinct) roots of $p(\xi)$ are denoted by $\lambda_i \in \mathbb{E}$, $i = 1, \ldots, n$.

Crucial in our analysis is the following lemma.

Lemma 2.1. *Let $p(\xi) = \xi^n + p_{n-1}\xi^{n-1} + \cdots + p_0 \in \mathbb{F}[\xi]$, with $\mathbb{F}$ a field. Let $\mathbb{E}/\mathbb{F}$ be a finite field extension such that $p(\xi)$ splits over $\mathbb{E}$, i.e., $p(\xi) = \prod_{i=1}^{n}(\xi - \lambda_i)$, $\lambda_i \in \mathbb{E}$, $i = 1 \ldots n$. For the power sums, defined by*

$$s_k := \sum_{i=1}^{n} \lambda_i^k, \quad k \in \mathbb{Z}_+ \tag{5}$$

there holds that $s_k \in \mathbb{F}$ for $k \in \mathbb{Z}_+$.

Proof (*See [4]*). Let $C \in \mathbb{F}^{n\times n}$ be a matrix whose characteristic polynomial of C is $p(\xi)$, e.g., a companion matrix of $p(\xi)$. The roots of $p(\xi)$ are the eigenvalues of C, and more generally, the kth powers of the roots of $p(\xi)$ are the eigenvalues of C^k. There also holds that the power sum s_k is the trace of C^k. Since $C \in \mathbb{F}^{n\times n}$, it follows that $C^k \in \mathbb{F}^{n\times n}$ for $k \in \mathbb{Z}_+$. Therefore

$$s_k = \operatorname{trace}(C^k) \in \mathbb{F}\,, \quad \forall k \in \mathbb{Z}_+ \quad \square \tag{6}$$

2.1. Multiplicity one

Theorem 2.2. *Let $\mathbb{F}$ be a finite field. Let $p(\xi) \in \mathbb{F}[\xi]$ be a monic irreducible polynomial of degree n, and let $\mathfrak{B} = \{w\colon \mathbb{Z}_+ \to \mathbb{F} \mid p(\sigma)w = 0\}$. Then $\mathfrak{B}$ is an n-dimensional subspace of $\mathbb{F}^{\mathbb{Z}_+}$.*
Let $\mathbb{E}/\mathbb{F}$ be a finite field extension such that $p(\xi)$ splits over $\mathbb{E}$, i.e., $p(\xi) = \prod_{i=1}^{n}(\xi - \lambda_i)$, with $\lambda_i \in \mathbb{E}$, $i = 1 \ldots n$ the distinct roots of $p(\xi)$. Then there holds $w \in \mathfrak{B}$ if and only if w is of the form

$$w(k) = \sum_{i=1}^{n}(a_0 + a_1\lambda_i + \cdots + a_{n-1}\lambda_i^{n-1})(\lambda_i)^k \tag{7}$$

with $a_m \in \mathbb{F}$, $m = 0, \ldots, n-1$.

Proof. First we show that the dimension of behavior $\mathfrak{B}$ equals $\deg(p(\xi)) = n$. A solution of (2.2) is completely determined by its initial values $w(0), \ldots, w(n-1)$. Let $\bar{w}_m$ denote the solution of (2.2) with

$$\bar{w}_m(k) = \begin{cases} 1 & \text{if } k = m \\ 0 & \text{if } k \neq m \end{cases} \quad m = 0, \ldots, n-1 \tag{8}$$

then $\mathfrak{B}$ is spanned by $\bar{w}_0, \ldots, \bar{w}_m$. The solutions $\bar{w}_m$, $m = 0, \ldots, n-1$ are obviously linearly independent.

Next we prove the *if* part. We have to show that if w is given by (7) then $w(k) \in \mathbb{F}$ for all $k \in \mathbb{Z}_+$. Expression (7) can be rewritten as

$$w(k) = \sum_{m=0}^{n-1} a_m \sum_{i=1}^{n} \lambda_i^{k+m}, \quad \text{with } a_m \in \mathbb{F},\ m = 0, \ldots, n-1. \tag{9}$$

It follows from Lemma 2.1 that $\sum_{i=1}^{n} \lambda_i^k \in \mathbb{F}$ for all $k \in \mathbb{Z}_+$. The statement follows.

It remains to show that w satisfies $p(\sigma)w = 0$. This is identical to the real or complex case. We skip the details.

To show the *only if* part, that is, all trajectories in $\mathfrak{B}$ are of the form (7), it suffices to prove that the zero solution in (7) can only be obtained by $a_j = 0$, $i = 0, \ldots, n-1$. Now, since the trajectories λ_i^k are linearly independent, it follows that to obtain the zero solution there must hold

$$a_0 + a_1\lambda_i + \cdots + a_{n-1}\lambda_i^{n-1} \quad i = 1, \ldots, n. \tag{10}$$

In matrix notation:

$$\begin{bmatrix}\alpha_0 & \alpha_1 & \cdots & \alpha_{n-1}\end{bmatrix}\underbrace{\begin{bmatrix}1 & 1 & \cdots & 1\\ \lambda_1 & \lambda_2 & \cdots & \lambda_n\\ \vdots & & & \vdots\\ \lambda_1^{n-1} & \lambda_2^n & \cdots & \lambda_n^{n-1}\end{bmatrix}}_{V} = 0. \tag{11}$$

Matrix $V \in \mathbb{E}^{n\times n}$ is a Vandermonde matrix and it follows that $a_0 = \ldots a_{n-1} = 0$. Hence there exist n linearly independent solutions of the form (7). Since $\dim \mathfrak{B} = n$ it follows that all solutions are of the form (7). □

2.2. Multiplicity larger than one

We now study the behavior corresponding to $p(\xi)^m$ where $p(\xi) \in \mathbb{F}[\xi]$ is irreducible and $m \in \mathbb{N}$. Let $\mathbb{E}$ be the splitting field of $p(\xi)$, then the roots $\lambda_i \in \mathbb{E}$ all have multiplicity m.

Theorem 2.3. *Let $\mathbb{F}$ be a finite field. Let $p(\xi) \in \mathbb{F}[\xi]$ be an irreducible monic polynomial of degree n and with $p(0) \neq 0$. Let $\mathfrak{B} = \{w\colon \mathbb{Z}_+ \to \mathbb{F} \mid p(\sigma)^m w = 0\}$. Then $\mathfrak{B}$ is an mn-dimensional subspace of $\mathbb{F}^{\mathbb{Z}_+}$. Let $\mathbb{E}/\mathbb{F}$ be a finite field extension such that $p(\xi)$ splits over $\mathbb{E}$. Denote the distinct roots of $p(\xi)$ by $\lambda_i \in \mathbb{E}$, $i = 1 \ldots n$. Then there holds $w \in \mathfrak{B}$ if and only if w of the form*

$$w(k) = \sum_{j=0}^{m-1} k^j \left[\sum_{i=1}^{n}\left(\sum_{\ell=0}^{n-1} a_{\ell j}\lambda_i^{\ell}\right)\lambda_i^k\right] \tag{12}$$

with $a_{\ell j} \in \mathbb{F}$, $\ell = 0, \ldots, n-1, j = 1 \ldots n$.

Proof. The dimension statement and the claim that all trajectories are of the form (12) follow from [2, Theorem 2.13]. The only difference between (7) and (12) is the factors k^j. As a consequence, just like in Theorem 2.3 we can conclude that $w(k) \in \mathbb{F}$.

What remains to show is that there exist nm linearly independent solutions of the form (12). To that end it suffices to prove that the zero solution in (12) can only be obtained by taking the coefficients $a_{\ell j} = 0$. This follows immediately from the fact that in $\mathbb{E}$ the trajectories $k^j\lambda_i^k$, $j = 0, \ldots, m-1$, $i = 1, \ldots, n$ are linearly independent. It follows that for $j = 0, \ldots, m-1$

$$\sum_{\ell=0}^{n-1} a_{\ell j}\lambda_i^{\ell} = 0.$$

Just like in the proof of Theorem 2.2 this implies that $a_{\ell j} = 0$. □

Remark 2.4. At the cost of a more complicated form of (12) involving the Hasse derivative, Theorem 2.3 also holds for the case that zero is a (multiple) root of $p(\xi)$.

3. Multivariable autonomous systems

We consider the multivariable autonomous system $\Sigma = (\mathbb{Z}_+, \mathbb{F}^q, \mathfrak{B})$ with $\mathbb{F}$ a finite field. The behavior $\mathfrak{B}$ is given by

$$P(\sigma)w = 0 \tag{13}$$

with $P(\xi) \in \mathbb{F}^{q\times q}[\xi]$ and $\det P(\xi) \neq 0$. Let $\chi(\xi) = \det(P(\xi))$ be the corresponding characteristic polynomial and n the degree of $\chi(\xi)$. Using the Smith form of $P(\xi)$, [5], it is easy to see that the behavior can be written as a direct sum of sub behaviors corresponding to the irreducible factors of $\chi(\xi)$. So just like for the scalar case we may treat the irreducible factors of $\chi(\xi)$ independently and

we therefore assume that $\chi(\xi)$ is a power of an irreducible factor. We first treat the multiplicity one case, i.e., $\chi(\xi)$ is irreducible. Let $\mathbb{E}$ be an extension field of $\mathbb{F}$ such that $\chi(\xi)$ splits over $\mathbb{E}$.

$$\chi(\xi) = \prod_{i=1}^{n}(\xi - \lambda_i) \quad \text{with } \lambda_i \in \mathbb{E}$$

where the $\lambda_1, \ldots, \lambda_n$ are mutually distinct.

Since each characteristic value λ_i is a simple root of $\chi(\xi)$ in $\mathbb{E}$, the kernel of $P(\lambda_i) \in \mathbb{E}^{q\times q}$ is one-dimensional.

Theorem 3.1. *There exists a nonzero polynomial vector $v(\xi) \in \mathbb{F}^q[\xi]$ such that*

$$\ker_{\mathbb{E}} P(\lambda_i) = \operatorname{span}_{\mathbb{E}}\{v(\lambda_i)\}$$

where λ_i, $i = 1, \ldots, n$ are the distinct roots of $\det P(\xi)$.

Proof. First we show that there exists a polynomial vector $v(\xi)$ such that $v(\lambda_i) \neq 0$ and $P(\lambda_i)v(\lambda_i) = 0$ for $i = 1, \ldots, n$. Polynomial matrix $P(\xi)$ can be transformed into Smith form, [5]. That is, there exist unimodular matrices $U(\xi)$, $V(\xi) \in \mathbb{F}^{q\times q}[\xi]$ such that

$$U(\xi)P(\xi)V(\xi) = D(\xi)$$

with $D(\xi)$ a diagonal matrix $D(\xi) = \operatorname{diag}(d_1(\xi), d_2(\xi), \ldots, d_q(\xi))$, where $d_i(\xi)$, $i = 1, \ldots, q$ are monic polynomials in $\mathbb{F}[\xi]$ and $d_i(\xi)$ divides $d_{i+1}(\xi)$. Because $\det P(\xi) \neq 0$, there holds $d_i(\xi) \neq 0$ for $i = 1, \ldots, q$. The roots of $\det P(\xi)$ in extension field $\mathbb{E}$ are simple. This implies that $D(\xi)$ is given by

$$D(\xi) = \operatorname{diag}(1, \ldots, 1, \chi(\xi))$$

Define $v(\xi)$ as the last column of $V(\xi)$, that is

$$v(\xi) = V(\xi)u \quad \text{with } u = \begin{bmatrix}0 & 0 & \cdots & 0 & 1\end{bmatrix}^T$$

then

$$\begin{aligned} P(\xi)v(\xi) &= U^{-1}(\xi)D(\xi)V^{-1}(\xi)V(\xi)u = U^{-1}(\xi)D(\xi)u \\ &= U^{-1}(\xi)\begin{bmatrix}0 & 0 & \cdots & 0 & \chi(\xi)\end{bmatrix}^T \end{aligned}$$

For every λ_i, $i = 1, \ldots, n$ holds $P(\lambda_i)v(\lambda_i) = 0$ and $v(\lambda_i) = V(\lambda_i)u \neq 0$ because $V(\xi)$ is unimodular. The determinant of $V(\lambda_i)$ is nonzero, so the last column of $V(\lambda_i)$ has nonzero elements.

Now we show that $\ker_{\mathbb{E}} P(\lambda_i) = \operatorname{span}_{\mathbb{E}}\{v(\lambda_i)\}$.

Let $P(\lambda_i)\tilde{v} = 0$ then $U^{-1}(\lambda_i)D(\lambda_i)V^{-1}(\lambda_i)\tilde{v} = 0$. So $D(\lambda_i)V^{-1}(\lambda_i)\tilde{v} = 0$. This means that $V^{-1}(\lambda_i)\tilde{v} = \begin{bmatrix}0, \ldots, 0, c\end{bmatrix}^T$ and thus $\tilde{v} = cv(\lambda_i)$ for some $c \in \mathbb{E}$. □

The multivariable version of Theorem 2.2 is:

Theorem 3.2. *Let $P(\xi) \in \mathbb{F}^{q\times q}[\xi]$, $\chi(\xi) = \det(P(\xi))$ irreducible with $\lambda_1, \ldots, \lambda_n$ the (distinct) roots of $\chi(\xi)$ in some extension field $\mathbb{E}$. Let $v(\xi) \in \mathbb{F}^q[\xi]$ be a polynomial vector such that $\ker_{\mathbb{E}} P(\lambda_i) = \{v(\lambda_i)\}$. Then $w \in \mathfrak{B}$, i.e., $P(\sigma)w = 0$, if and only if w is of the form*

$$w(k) = \sum_{i=1}^{n}(a_0 + a_1\lambda_i + \cdots + a_{n-1}\lambda_i^{n-1})v(\lambda_i)(\lambda_i)^k \tag{14}$$

with $a_i \in \mathbb{F}$, $i = 0, \ldots, n-1$.

Lemma 3.3. *Let w be given by (14). If $a_j \in \mathbb{F}$, $j = 1, \ldots, n$ then $w(k) \in \mathbb{F}^q$ for all $k \in \mathbb{Z}_+$.*

Proof. Let r be the maximum row degree of polynomial vector $v(\xi)$. Then $v(\xi)$ can be written as

$$v(\xi) = \sum_{j=0}^{r} v_j \xi^j, \quad \text{with } v_j \in \mathbb{F}^q, j = 0, \ldots, r$$

Rewriting (14) yields

$$\begin{aligned} w(k) &= \sum_{i=1}^{n} \left[\left(\sum_{m=0}^{n-1} a_m \lambda_i^m \right) \left(\sum_{j=0}^{r} v_j \lambda_i^j \right) (\lambda_i)^k \right] \\ &= \sum_{i=1}^{n} \sum_{j=0}^{r} \sum_{m=0}^{n-1} a_m v_j \lambda_i^{m+j+k} \\ &= \sum_{j=0}^{r} \sum_{m=0}^{n-1} a_m v_j \left(\sum_{i=1}^{n} \lambda_i^{m+j+k} \right) \end{aligned}$$

Because for $m = 0, \ldots, n-1, j = 0, \ldots, n-1$, and for all $k \in \mathbb{Z}_+$ holds $a_m \in \mathbb{F}$, $v_j \in \mathbb{F}^q$ and, by Lemma 2.1, $\sum_{i=1}^{n} \lambda_i^{m+j+k} \in \mathbb{F}$. It follows that $w(k) \in \mathbb{F}^q$ for all $k \in \mathbb{Z}_+$. □

Lemma 3.4. *Let w be given by (14) then there holds $P(\sigma)w = 0$.*

Proof.

$$\begin{aligned} P(\sigma)w(k) &= P(\sigma) \sum_{i=1}^{n} (a_0 + a_1\lambda_i + \cdots + a_{n-1}\lambda_i^{n-1}) v(\lambda_i)(\lambda_i)^k \\ &= \sum_{i=1}^{n} (a_0 + a_1\lambda_i + \cdots + a_{n-1}\lambda_i^{n-1}) P(\sigma) \left(v(\lambda_i)(\lambda_i)^k \right) \\ &= \sum_{i=1}^{n} (a_0 + a_1\lambda_i + \cdots + a_{n-1}\lambda_i^{n-1}) P(\lambda_i) v(\lambda_i)(\lambda_i)^k \\ &= 0 \quad \square \end{aligned}$$

Lemma 3.5. *Behavior $\mathfrak{B}$ has dimension n.*

Proof. Let $U(\xi)D(\xi)V(\xi)$ be the Smith form decomposition of $P(\xi)$: $D(\xi) = \operatorname{diag}(1 \cdots 1\ \chi(\xi))$ and $U(\xi)$ and $V(\xi)$ are unimodular matrices. Let $\tilde{\mathfrak{B}}$ be the behavior defined by

$$\tilde{\mathfrak{B}} = \{\tilde{w} \colon \mathbb{Z}_+ \to \mathbb{F}^q \mid D(\sigma)\tilde{w} = 0\}.$$

It is obvious that $\tilde{w} \in \mathfrak{B}$ if and only if $\tilde{w} = (0, \ldots, 0, \tilde{w}_n)$ where $\tilde{w}_n$ is a solution of the scalar differential equation

$$\chi(\sigma)\tilde{w}_n = 0. \tag{15}$$

It follows from Theorem 2.2 that $\tilde{\mathfrak{B}}$ has dimension n. Now let $\tilde{w} \in \tilde{\mathfrak{B}}$ then $w = V^{-1}(\sigma)\tilde{w} \in \mathfrak{B}$ because $P(\sigma)w = U(\sigma)D(\sigma)V(\sigma)V^{-1}(\sigma)\tilde{w} = U(\sigma)D(\sigma)\tilde{w} = 0$ Also if $w \in \mathfrak{B}$ then $\tilde{w} = V(\sigma)w \in \tilde{\mathfrak{B}}$ because $D(\sigma)\tilde{w} = U^{-1}(\sigma)P(\sigma)V^{-1}(\sigma)V(\sigma)w = U^{-1}(\sigma)P(\sigma)w = 0$. So $V(\sigma)$ defines an isomorphism between $\mathfrak{B}$ and $\tilde{\mathfrak{B}}$. Therefore $\mathfrak{B}$ has the same dimension as $\tilde{\mathfrak{B}}$, that is, n. □

We can rewrite Eq. (14) as a linear combination

$$w(k) = \sum_{m=0}^{n-1} a_m w_m(k) \quad \text{with } a_0, \ldots, a_{n-1} \in \mathbb{F} \quad \text{and} \tag{16}$$

$$w_m(k) := \sum_{i=1}^{n} v(\lambda_i)\lambda_i^{k+m} \quad m = 0, \ldots, n-1, k \in \mathbb{Z}_+ \tag{17}$$

It follows from Lemmas 3.3 and 3.4 that $w_0, \ldots, w_{n-1}$ are elements of $\mathfrak{B}$.

Lemma 3.6. *The trajectories defined by (14) span an n-dimensional sub-space.*

Proof. Just like in the scalar case it suffices to prove that the zero trajectory can be obtained from (14) only by taking the coefficients $a_i = 0$. So let

$$\sum_{i=1}^{n}(a_0 + a_1\lambda_i + \cdots + a_{n-1}\lambda_i^{n-1})v(\lambda_i)(\lambda_i)^k = 0 \quad \forall k \tag{18}$$

Since for each i $v(\lambda_i) \neq 0$ we can read the q-dimensional system of equations (18) line by line to conclude that $(a_0 + a_1\lambda_i + \cdots + a_{n-1}\lambda_i^{n-1}) = 0$ for all i. It follows that $a_0 = \cdots = a_{n-1} = 0$. □

Proof (*Theorem 3.2*). The *if* part follows from Lemmas 3.3 and 3.4.
The *only if* part goes as follows. From Lemma 3.5 it follows that $\dim \mathfrak{B} = n$. Lemma 3.6 and (17) show that $w_0, \ldots, w_{n-1}$ are n linearly independent solutions in $\mathfrak{B}$. It follows that $\mathfrak{B}$ is spanned by those solutions. So any solution $w \in \mathfrak{B}$ can be written as in (16), that is, as in (14). □

3.1. Higher multiplicity

Key in the multivariable case, multiplicity one, is Theorem 3.1. If the characteristic polynomial of $P(\xi)$ contains powers of irreducible factors, that is, some of its roots have multiplicity larger than one, the situation becomes increasingly more complicated. In principle, however, Theorem 3.1 may be generalized for arbitrary multiplicities. To keep the discussion transparent, we only treat the multiplicity two case.

Theorem 3.7. *Let $P(\xi) \in \mathbb{F}^{q\times q}[\xi]$ such that $\det P(\xi) = p(\xi)^2$, with $p(\xi) \in \mathbb{F}[\xi]$ monic of degree n and irreducible and $p(0) \neq 0$. Denote the distinct roots of $p(\xi)$ by $\lambda_i \in \mathbb{E}$, $i = 1, \ldots, n$. Let $\mathfrak{B} = \{w : \mathbb{Z}_+ \to \mathbb{F}^q \mid P(\sigma)w = 0\}$.*

(1) There exists a matrix $C(\xi) \in \mathbb{F}^{2q\times 2}[\xi]$ such that:

$$\begin{bmatrix} P(\lambda_i) & P'(\lambda_i) \\ 0 & P(\lambda_i) \end{bmatrix} C(\lambda_i) = 0, \quad i = 1, \ldots, n, \tag{19}$$

and the columns of $C(\lambda_i)$ are linearly independent for $i = 1, \ldots, n$.

(2) Partition $C(\xi)$ as:

$$C(\xi) = \begin{bmatrix} C_{01}(\xi) & C_{02}(\xi) \\ C_{11}(\xi) & C_{12}(\xi) \end{bmatrix},$$

with $C_{\ell_1\ell_2} \in \mathbb{F}^{q\times 1}[\xi]$. Then $w \in \mathfrak{B}$ if and only if

$$\begin{aligned} w(k) = \sum_{i=1}^{n}\Big[&(a_0 + a_1\lambda_i + \cdots + a_{n-1}\lambda_i^{n-1})(C_{01}(\lambda_i)\lambda_i^k + C_{11}(\lambda_i)k\lambda_i^k) \\ &+(b_0 + b_1\lambda_i + \cdots + b_{n-1}\lambda_i^{n-1})(C_{02}(\lambda_i)\lambda_i^k + C_{12}(\lambda_i)k\lambda_i^k)\Big], \end{aligned}$$

with $a_j, b_j \in \mathbb{F}$.

Proof. (1) Let $U(\xi), V(\xi) \in \mathbb{F}^{q\times q}[\xi]$ such that $D(\xi) = U(\xi)P(\xi)V(\xi)$ is the Smith form of $P(\xi)$. As $U(\xi)$ is immaterial in this context, we assume, without loss of generality, that $U(\xi) = I_q$. In view of Theorem 1.1, the elements of $\mathfrak{B}$ are of the form (1) where the coefficients satisfy the linear relations (2). For our case, multiplicity two, the coefficients are related to the kernel of

$$\begin{bmatrix} P(\lambda_i) & P'(\lambda_i) \\ 0 & P(\lambda_i) \end{bmatrix}, \tag{20}$$

where $P'(\xi)$ denotes the formal derivative of $P(\xi)$. It is straightforward to verify that

$$\begin{bmatrix} P(\lambda_i) & P'(\lambda_i) \\ 0 & P(\lambda_i) \end{bmatrix} \begin{bmatrix} V(\lambda_i) & V'(\lambda_i) \\ 0 & V(\lambda_i) \end{bmatrix} = \begin{bmatrix} D(\lambda_i) & D'(\lambda_i) \\ 0 & D(\lambda_i) \end{bmatrix}. \tag{21}$$

Since λ_i is a root of $\det(P(\xi))$ of multiplicity two, it follows that there are two possibilities for $D(\xi)$:

$$D(\xi) = \operatorname{diag}\begin{bmatrix} 1 & \cdots & 1 & p(\xi)^2 \end{bmatrix} \text{ or } D(\xi) = \operatorname{diag}\begin{bmatrix} 1 & \cdots & 1 & p(\xi) & p(\xi) \end{bmatrix}. \tag{22}$$

In both cases the right-hand side of (21) has a rank deficiency of two which proves the statement.

Depending in which form $D(\xi)$ takes, we define $C(\xi)$ as

$$C(\xi) = \begin{bmatrix} V(\xi) & V'(\xi) \\ 0 & V(\xi) \end{bmatrix} \begin{bmatrix} e_q & 0 \\ 0 & e_{2q} \end{bmatrix}, \quad C(\xi) = \begin{bmatrix} V(\xi) & V'(\xi) \\ 0 & V(\xi) \end{bmatrix} \begin{bmatrix} e_{q-1} & e_q \\ 0 & 0 \end{bmatrix} \tag{23}$$

respectively. Here e_i denotes the ith unit vector in $\mathbb{F}^{2q}$.

(2) This follows along the same lines as the proof of Theorem 3.2. □

Remark 3.8. Theorem 3.7 may be generalized for higher multiplicities without any difficulties, except that the formulas become highly complicated. Also, it should be noted that in the case of finite fields the formal derivatives should be replaced by the Hasse derivative. Furthermore, using Hasse derivative the condition that $p(0) \neq 0$ may be relaxed.

Example 3.9. Consider the system $\Sigma(\mathbb{Z}_+, \mathbb{Z}_p^q, \mathfrak{B})$, with $p = 5$, $q = 2$ and the behavior given by

$$P(\sigma)w = 0, \quad \text{with } P(\xi) = \begin{bmatrix} 1 & 3\xi^2 + 1 \\ 3\xi & 4\xi + 1 \end{bmatrix}$$

The determinant is

$$\det P(\xi) = (4\xi + 1) - (3\xi^2 + 1)(3\xi) = \xi^3 + \xi + 1$$

This polynomial is monic, the characteristic polynomial is therefore $\chi(\xi) = \xi^3 + \xi + 1$. The 3rd degree polynomial $\chi(\xi)$ has no roots in $\mathbb{Z}_5$ and hence is irreducible over $\mathbb{Z}_5$.

In field extension $\mathbb{E} = \mathbb{Z}_5(\lambda)$, with λ defined as a root of $\chi(\xi)$, the roots of $\chi(\xi)$ are given by

$$\lambda_1 = \lambda$$
$$\lambda_2 = \lambda^5 = \lambda^2(\lambda^3) = \lambda^2(4\lambda + 4) = 4\lambda^3 + 4\lambda^2 = 4\lambda^2 + \lambda + 1$$
$$\lambda_3 = \lambda^{25} = \cdots = \lambda^2 + 3\lambda + 4$$

The kernel of $P(\lambda)$ is $\{v(\lambda)\}$ with $v(\lambda) = \begin{bmatrix} 4\lambda + 1 & -3\lambda \end{bmatrix}^T \sim \begin{bmatrix} 4\lambda + 1 & 2\lambda \end{bmatrix}^T$. To verify this we calculate $P(\lambda)v(\lambda)$.

$$\begin{bmatrix} 1 & 3\lambda^2 + 1 \\ 3\lambda & 4\lambda + 1 \end{bmatrix} \begin{bmatrix} 4\lambda + 1 \\ 2\lambda \end{bmatrix} = \begin{bmatrix} 6\lambda^3 + 6\lambda + 1 \\ 20\lambda^2 + 5\lambda \end{bmatrix} = \begin{bmatrix} \lambda^3 + \lambda + 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Substituting λ_1, λ_2 and λ_3 yields

$$v(\lambda_1) = \begin{bmatrix} 4\lambda + 1 \\ 2\lambda \end{bmatrix}, \quad v(\lambda_2) = \begin{bmatrix} \lambda^2 + 4\lambda \\ 3\lambda^2 + 2\lambda + 2 \end{bmatrix}, \quad v(\lambda_3) = \begin{bmatrix} 4\lambda^2 + 2\lambda + 2 \\ 2\lambda^2 + \lambda + 3 \end{bmatrix}$$

The general solution of $P(\sigma)w = 0$ is given by

$$w(k) = \sum_{i=1}^{3}(a_0 + a_1\lambda_i + a_2\lambda_i^2)v(\lambda_i)(\lambda_i)^k \quad \text{with } a_0, a_1, a_2 \in \mathbb{Z}_5.$$

We could have derived another polynomial $v(\xi)$ by bringing $P(\xi)$ into Smith form, using Theorem 3.1. There holds that

$$\underbrace{\begin{bmatrix} 1 & 0 \\ 2\xi & 1 \end{bmatrix}}_{U(\xi)} \underbrace{\begin{bmatrix} 1 & 3\xi^2+1 \\ 3\xi & 4\xi+1 \end{bmatrix}}_{P(\xi)} \underbrace{\begin{bmatrix} 1 & 2\xi^2+4 \\ 0 & 1 \end{bmatrix}}_{V(\xi)} = \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & \xi^3+\xi+1 \end{bmatrix}}_{D(\xi)}$$

Take $v(\xi) = V_{*2}(\xi) = \begin{bmatrix} 2\xi^2+4 \\ 1 \end{bmatrix}$. Note that $2\lambda v(\lambda) = \cdots = \begin{bmatrix} 4\lambda+1 \\ 2\lambda \end{bmatrix}$.

Remark 3.10. All results derived in this paper have counterparts for the case that the time axis is $\mathbb{Z}$ rather than $\mathbb{Z}_+$. The underlying polynomial ring then is $\mathbb{F}[\xi, \xi^{-1}]$. The degree of a polynomial $P(\xi, \xi^{-1})$ is defined as the difference between the largest and smallest exponent. For instance $\deg \xi + \xi^{-1} = 2$. With this definition of degree all results remain valid except that $\lambda = 0$ can not be a characteristic value.

4. Conclusions

We have obtained a complete time-domain description of the behavior represented by systems of higher order difference equations over finite fields. This was achieved by first computing the behavior in a suitable extension field and subsequently restricting the extended behavior to the base field. It should be noted that alternatively one could also derive expressions through a state space representation of the behavior. However, this is an indirect way that yields less transparent expressions. In particular the role of the characteristic values will be somewhat hidden.

References

[1] R. van de Kreeke, J.W. Polderman, Time-domain description of behaviors over finite fields, in: Proceedings of the 18th International Symposium on Mathematical Theory of Networks and Systems, Blacksburg, Virginia, USA, Virginia Tech, Blacksburg, 2008.
[2] M. Kuijper, J. Polderman, R-S list decoding from a system theoretic perspective, IEEE Trans. Inform. Theory 50 (2004) 259–271.
[3] R. Lidl, H. Niederreiter, Finite Fields, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997. (with a foreword by P.M. Cohn).
[4] D. Kalman, A matrix proof of Newton's identities, Math. Mag. 73 (2000) 315–333.
[5] J.W. Polderman, J.C. Willems, Introduction to Mathematical System Theory: A Behavioral Approach, Texts in Applied Mathematics, vol. 26, Springer, New York, NY, USA, 1997.